RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Garbanzo ("Service Provider") on 08/30/2024 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ● No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ● No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ● No ○

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ◉ No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ◉ No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ◉ No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ◉ No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ◉ No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ◉ No ○

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ● No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ● No ○

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ● No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ● No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ● No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ● No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ● No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ● No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ● No ○

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ● No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ● No ○

3. Vendors cannot sell student information.

   Agree: Yes ● No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ● No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ● No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ● No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ● No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

Samantha Brumagin 8.30.24
Print Name

Samantha Brumagin
Signature, Date

Laura Assem
Print Name (Roseville City School District)

08/30/2024
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Section 1.7: Internal Security

Section II.2: Exporting of Student-Created Content

Section II.4: Review and Correcting Personally Identifiable Information (PII)

EXHIBITS

Section II.5: Securing Student Data

Section II.6: Disclosure Notification

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Section III.5: How Student Data is Protected:

Reset Form

Garbanzo LLC’s

Report on Description of its System and Organization Controls (SOC 2 Type 2) related to the Garbanzo Software Application and on the Suitability of the Design and Operating Effectiveness of controls relevant to Security, Availability and Confidentiality Trust Service Criteria for the period from February 28, 2024 to June 06, 2024.

Statement of Confidentiality

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of the Service Organization, User Entities of the Service Organization's system related to the Garbanzo Software Application relevant to Security, Availability and Confidentiality for the period from February 28, 2024 to June 06, 2024, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties. Unauthorized use, reproduction or distribution of this report, in whole or in part, is strictly prohibited.

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR’S REPORT

1. Independent Service Auditors' Report

Independent Service Auditors' Report on Description of Garbanzo LLC's System and the Suitability of the Design and Operating Effectiveness of Controls relevant to Security, Availability and Confidentiality trust service criteria.

To the Management of Garbanzo LLC

Scope

We have examined Garbanzo LLC's (the "Service Organization" or "Garbanzo LLC") accompanying System Description Provided by Service Organization of its system for the Garbanzo Software Application for the period from February 28, 2024 to June 06, 2024 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description for the period from February 28, 2024 to June 06, 2024 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Garbanzo LLC uses AWS and Digital Ocean ("Subservice Organization") as cloud service providers. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Garbanzo LLC, to achieve Garbanzo LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Garbanzo LLC' system; its controls; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at subservice organization. Our examination did not extend to the services provided by subservice organization and we have not evaluated whether the controls management assumes have been implemented at subservice organization have been implemented or whether such controls were suitably designed and operating effectively for the period from February 28, 2024 to June 06, 2024.

The Description also indicates that Garbanzo LLC's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Garbanzo LLC's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Garbanzo LLC's responsibilities

Garbanzo LLC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved. Garbanzo LLC has provided the accompanying assertion titled, Garbanzo LLC's Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Garbanzo LLC is responsible for: (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the Service Organization's service commitments and system requirements, based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system and the service organization's service commitments and system requirements
- performing procedures to obtain evidence about whether the controls stated in the Description are presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively based on the applicable trust services criteria.
- testing the operating effectiveness of those controls based on the applicable trust services criteria.
- evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances. We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements related to the examination engagement.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, except for the effects of the matters giving rise to the modification, in all material respects:

a. the Description presents the system that was designed and implemented for the period from February 28, 2024 to June 06, 2024 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively [and if the subservice organization(s)] and user entities applied the controls assumed in the design of Garbanzo LLC's controls for the period from February 28, 2024 to June 06, 2024.

c. The controls operated effectively to provide reasonable assurance that the Applicable Trust Services Criteria were met for the period from February 28, 2024 to June 06, 2024. If complementary user entity controls contemplated in the design of the Service Organization's controls operated effectively for the period from February 28, 2024 to June 06, 2024.

Restricted Use

This report, including the Description of tests of controls and results thereof in Section IV is intended solely for the information and use of Garbanzo LLC, user entities of the Service Organization's using the Garbanzo Software Application relevant to the Security, Availability and Confidentiality for the period from February 28, 2024 to June 06, 2024, and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization.
- How the Service Organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and how they interact with related controls at the Service Organization to meet the Applicable Trust Services Criteria.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The Applicable Trust Services Criteria.
- The risks that may threaten the achievement of the Applicable Trust Services Criteria and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

For,

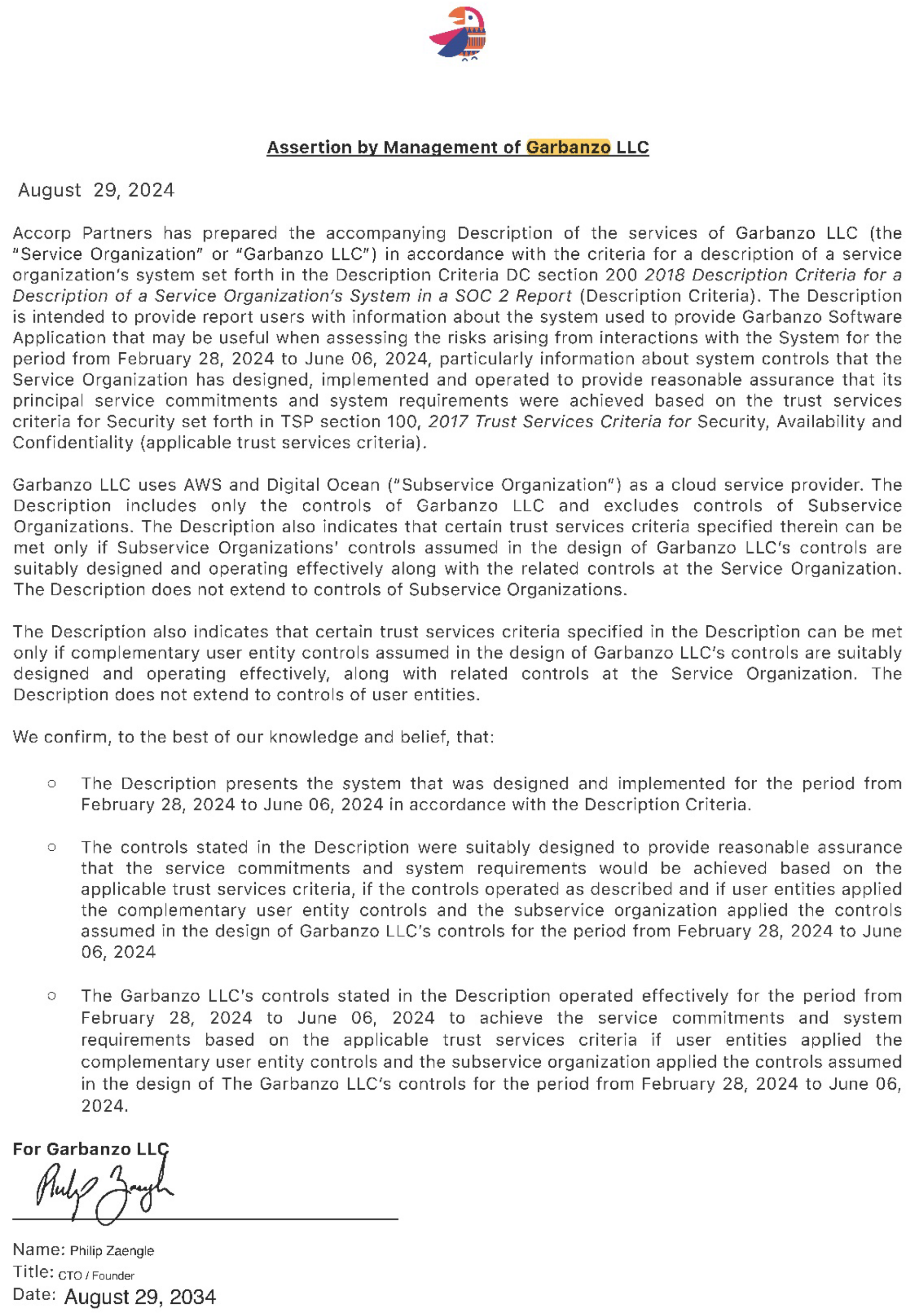
Accorp Partners CPA LLC

Accorp Partners CPA LLC
License no: PAC-FIRM-LIC-47383
Date: August 30, 2024

SECTION 2

MANAGEMENT ASSERTION PROVIDED BY SERVICE ORGANIZATION

2. Assertion by Management of Garbanzo LLC



Assertion by Management of Garbanzo LLC

August 29, 2024

Accorp Partners has prepared the accompanying Description of the services of Garbanzo LLC (the "Service Organization" or "Garbanzo LLC") in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the system used to provide Garbanzo Software Application that may be useful when assessing the risks arising from interactions with the System for the period from February 28, 2024 to June 06, 2024, particularly information about system controls that the Service Organization has designed, implemented and operated to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the trust services criteria for Security set forth in TSP section 100, *2017 Trust Services Criteria for* Security, Availability and Confidentiality (applicable trust services criteria).

Garbanzo LLC uses AWS and Digital Ocean ("Subservice Organization") as a cloud service provider. The Description includes only the controls of Garbanzo LLC and excludes controls of Subservice Organizations. The Description also indicates that certain trust services criteria specified therein can be met only if Subservice Organizations' controls assumed in the design of Garbanzo LLC's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of Subservice Organizations.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Garbanzo LLC's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of user entities.

We confirm, to the best of our knowledge and belief, that:

- ○ The Description presents the system that was designed and implemented for the period from February 28, 2024 to June 06, 2024 in accordance with the Description Criteria.
- ○ The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of Garbanzo LLC's controls for the period from February 28, 2024 to June 06, 2024
- ○ The Garbanzo LLC's controls stated in the Description operated effectively for the period from February 28, 2024 to June 06, 2024 to achieve the service commitments and system requirements based on the applicable trust services criteria if user entities applied the complementary user entity controls and the subservice organization applied the controls assumed in the design of The Garbanzo LLC's controls for the period from February 28, 2024 to June 06, 2024.

For Garbanzo LLC

Name: Philip Zaengle
Title: CTO / Founder
Date: August 29, 2034

SECTION 3

DESCRIPTION OF THE SYSTEM

3. System Description Provided by Service Organization

3.1 Overview of the Company and Services Delivered of the Report

Garbanzo is a cloud-hosted software application built by Garbanzo LLC hereby referred to as Garbanzo.

Garbanzo is an online language-learning platform

Any other services provided by Garbanzo LLC are not in the scope of this report.

3.2 Components of the System used to provide services

Infrastructure & Network Architecture

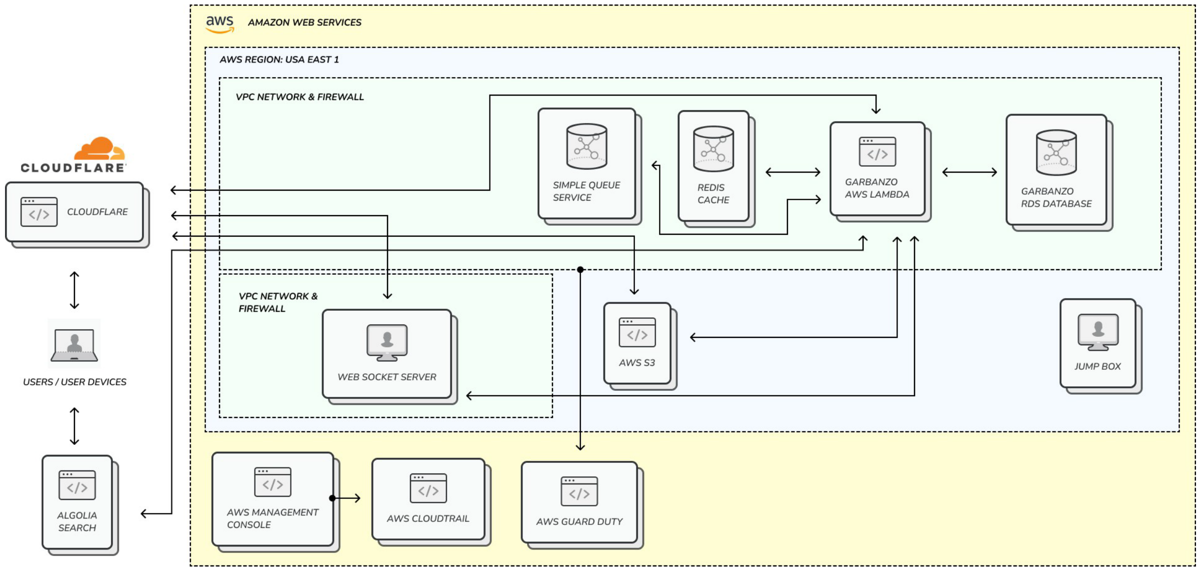
The production infrastructure for the Garbanzo software application is hosted on AWS and Digital Ocean, Digital Ocean in their various regions across US East.

Garbanzo software application uses a virtual and secure network environment on top of AWS and Digital Ocean, Digital Ocean infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. Garbanzo software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through the AWS and Digital Ocean, Digital Ocean Internet Gateway, over to a Virtual Private Cloud that:

1. Houses the entire application runtime
2. Protects the application runtime from any external networks

The internal networks of AWS and Digital Ocean, Digital Ocean are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through.



Software

Garbanzo LLC is responsible for managing the development and operation of the Garbanzo platform including infrastructure components such as servers, databases, and storage systems. The in-scope Garbanzo infrastructure and software components are shown in the table below:

Primary Infrastructure and Software			
System / Application	**Business Function / Description**	**Underlying Operating System & Storage**	**Physical Location**
Garbanzo Application	Access to the Garbanzo SaaS application is through a web/mobile interface and user authentication.	AWS and Digital Ocean Lambda, PHP(Laravel), JavaScript (Vue), PGsql	AWS and Digital Ocean, Digital Ocean US East
AWS and Digital Ocean IAM	Identity and access management console for AWS and Digital Ocean resources.	AWS and Digital Ocean Proprietary	AWS and Digital Ocean
AWS and Digital Ocean Firewalls	Front-end firewalls protect the network perimeter with rule-based ACLs and back-end firewalls segregate the database servers from internal traffic.	AWS and Digital Ocean Proprietary	AWS and Digital Ocean
Git	Source code repository, version control system, and build software.	Git	Git Cloud
Google	Identity/Email provider for all Garbanzo LLC employees	Google Proprietary	Google

Supporting Tools	
System / Application	**Business Function / Description**
PHP, JavaScript	Programming Language used for Garbanzo application
Sprinto	Provide continuous compliance monitoring of the company's system.
Google	Office communication services

People

Garbanzo LLC’s staff have been organized into various functions like Sales, Support, Engineering, Product Management, etc. The personnel have also been assigned to the following key roles:

Senior Management: Senior management carries the ultimate responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization’s mission. They also assess and incorporate the results of the risk assessment activity into the decision-making process. The senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security program of the organization. Decisions made in these areas are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, and vulnerabilities, and adding controls to mitigate these risks. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member who would be responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of the effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines, and rules of behaviour is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members that access IT resources are provided with annual security awareness training.

Procedures and Policies

Formal policies and procedures have been established to support Garbanzo LLC software application. These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management

Via the Sprinto platform, all policies are made available to all staff members to provide direction regarding the staff members' responsibilities related to the functioning of internal control. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring (and annually thereafter).

Garbanzo LLC also provides information to clients and staff members on how to report failures, incidents, concerns, or complaints related to the services or systems provided by the Garbanzo Software Application, in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Data

Data, as defined by Garbanzo LLC, constitutes the following:

- Transaction data
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

All data that is managed, processed and stored as a part of the Garbanzo Software Application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization. All data is to be assigned one of the following sensitivity levels:

Data Sensitivity	Description	Examples
Customer confidential	Highly valuable and sensitive information where the level of protection is dictated internally through policy and externally by legal and/or contractual requirements. Access to confidential information is limited to authorized employees, contractors, and business partners with a specific need.	• Customer system and operating data • Customer PII • Anything subject to a confidentiality agreement with a customer
Company Confidential	Information that originated or is owned internally, or was entrusted to Garbanzo LLC by others. Company confidential information may be shared with authorized employees, contractors, and business partners but not released to the general public.	• Garbanzo LLC’s PII • Unpublished financial information • Documents and processes explicitly marked as confidential • Unpublished goals, forecasts, and initiatives marked as confidential • Pricing/marketing and other undisclosed strategies
Public	Information that has been approved for release to the public and is freely shareable both internally and externally.	• Press releases • Public website

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data backup policy.

Control Environment

Garbanzo LLC 's control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company’s objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Logical Access Control

Garbanzo Software Application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

Garbanzo LLC has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member as well as a role based access matrix prior to being issued system credentials and granted the ability to access the system. When a person is relieved of duties from the company, access to critical systems are revoked within three business days.

Administrator access to the production console is restricted to authorized system and security administrators. Powerful service/system accounts and keys are either restricted from direct user authentication or authorized to unique users through a password vault or equivalent security solution. Production infrastructure root level account usage is logged with alerting configured.

The Information Security Officer is responsible for performing quarterly reviews of everyone who has access to the system and assesses the appropriateness of the access and permission levels and make modifications based on the principle of least-privilege, whenever necessary.

Staff members must use complex passwords, wherever possible, for all of their accounts that have access to Garbanzo LLC customer data. Staff are encouraged to use passwords which have at least 10 characters, randomly generated, alphanumeric and special-character based. Password configuration settings are documented and systematically enforced based on the password complexity requirements configured on each critical system. Access to cloud services or remote access systems requires multi-factor authentication (MFA). Additionally, company owned endpoints are configured to auto-screen-lock after 15 minutes of inactivity.

Physical Access and Environmental Controls

The in-scope system and supporting infrastructure is hosted by AWS and Digital Ocean. As such AWS and Digital Ocean is responsible for the physical security controls of the in-scope system. Garbanzo LLC reviews the SOC 2 report provided by AWS and Digital Ocean on an annual basis, to ensure their controls are in accordance with standards expected by the customers of Garbanzo LLC software application.

Incident Management

Garbanzo LLC has an incident management framework that includes defined processes, roles, communications, responsibilities, and procedures for detection, escalation, and response to incidents internally and to customers. Customers are directed to contact Garbanzo LLC via the support email address provided during onboarding to report failures, incidents, concerns, or other complaints in the event there were problems.

Incident response procedures and centralized tracking tools consist of different channels for reporting production system incidents and weaknesses. Production infrastructure is configured to generate audit events for actions of interest related to operations and security. Security alerts are tracked, reviewed, and analyzed for anomalous or suspicious activity.

Where required, security incidents are escalated to privacy, legal, customer, or senior management team(s) and assigned a severity rating. Operational events are automatically resolved by the self-healing system.

- **Low severity incidents** are those that do not require immediate remediation. These typically include a partial service of Garbanzo LLC being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
- **Medium severity incidents** are similar to low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium severity incidents usually cover the large majority of incidents found.
- **High severity incidents** are problems an active security attack has not yet happened but is likely. This includes situations like backdoors, malware, malicious access of business data (e.g., passwords, payment information, vulnerability data, etc.). In such cases, the information security team must be informed and immediate remediation steps should begin.
- **Critical severity incidents** are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.

Post-mortem activities are conducted for incidents with critical severity ratings. Results of post-mortems may include updates to the security program or changes to systems required as a result of incidents.

Network Operations Monitoring

Web applications are protected by deploying network firewalls and security groups that inspect traffic flowing to the web application for common attacks. The network is segmented based on the label or classification level of the information stored on the servers. This includes filtering between virtual private cloud (VPC) environments to help ensure only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities. Operations and security functions use a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs.

Incidents and alerts from the security utilities are reviewed by Garbanzo LLC management. Security events requiring further investigation are tracked using internal ticketing systems and monitored until resolved.

Garbanzo LLC only uses network ports, protocols, and services listening on a system with validated business need to run on each system. Default-deny rules drop traffic except those services and ports that are explicitly allowed.

Cryptography

User requests to Garbanzo LLC’s systems are encrypted using Transport Layer Security (TLS) using certificates from an established third party certificate authority. Remote system administration access to Garbanzo LLC web and application servers is available through cryptographic network protocols (i.e., SSH) or an encrypted virtual private network (VPN) connection. Data at rest is encrypted using Advanced Encryption Standard (AES) 256 bit.

Change Management

A documented Change Management Policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to Garbanzo LLC's application and IT infrastructure are reviewed, deployed, and managed. The policy covers all changes made to the Garbanzo Software Application, regardless of their size, scope, or potential impact.

The Change Management Policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the Garbanzo Software Application can be initiated by a staff member with an appropriate role. Garbanzo LLC uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities.

Customer content and personal information are not used in non-production environments.

Software Security Assurance

Secure coding practices are established based on the programming language and development environment used. In-house developed software includes explicit error checking and documented inputs, including for size, data type, and acceptable ranges or formats. Security analysis is performed to verify secure coding practices are followed during change control. Vulnerabilities identified, if any, are tracked to resolution.

Asset Management (Hardware and Software)

Assets used in the system are inventoried or tagged to include business descriptions, asset ownership, versions, and other configuration levels, as appropriate, to help ensure assets are classified appropriately, patched, and tracked as part of configuration management. Garbanzo LLC uses tagging tools to automatically facilitate the company’s hardware and software asset inventory. This helps to ensure a complete and accurate inventory of technology assets with the potential to store or process information is maintained.

System Hardening, Vulnerability Management and Penetration Testing

Vulnerability scanning tools are used to automatically scan systems on the network at least monthly to identify potential vulnerabilities. Automated software update tools are used to help ensure operating systems are running the most recent security updates provided by the software vendor. Vulnerabilities identified are risk-ranked to prioritize the remediation of discovered vulnerabilities.

Endpoint Management

Endpoint management solutions are in place that include policy enforcement on company issued devices, as well as bring-your-own devices that could connect to or access data within the system boundaries. Policies enforced on endpoints include encryption on devices for data at rest.

To help prevent malware, the following are implemented within the organization:

- Email attachments entering the organization's email gateway are scanned for viruses; and,
- Anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

Availability

Garbanzo LLC has a documented business continuity plan (BCP) and testing performed against the recovery time objectives (RTOs) and recovery point objectives (RPOs). At least daily backup schedules are maintained to protect sensitive data from loss in the event of a system failure. Backups are restored at least annually as part of operational activities and are included as part of the BCP test plan.

3.3 Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Although the applicable trust services criteria and related controls are included in Section IV, they are an integral part of Garbanzo LLC’s description of the system. This section provides information about the five interrelated components of internal control at Garbanzo LLC, including

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring controls

3.4 Control Environment

Integrity & Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Garbanzo LLC’s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behaviour are the product of Garbanzo LLC’s ethical and behavioural standards, how they are communicated, and how they are reinforced in practices. They include management’s actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioural standards to personnel through policy statements and codes of conduct.

Garbanzo LLC and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented "Code of business conduct" communicates the organization's values and behavioural standards to staff members
- Staff members are required to acknowledge (upon hiring and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management, and Access Control. Staff Members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

Garbanzo LLC’s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees’ roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their job responsibilities at the time of hiring.

Management Philosophy and Operating Style

Garbanzo LLC’s management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management’s approach to monitoring business risks, and management’s attitudes toward personnel and the processing of information.

Garbanzo LLC’s information security function, composed of senior management and the Information Security Officer, meets frequently and includes at least an annual meeting to review policies and procedures and set the information security program roadmap. The security function, under the direction of senior management, oversees the security activities and communication of its policies and procedures.

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually

Organizational Structure and Assignment of Authority and Responsibility

Garbanzo LLC’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the Entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and are updated as required.

Human Resources Policies and Practices

Garbanzo LLC’s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by the management's ability to hire and retain top-quality personnel who ensure the service organization is operating at maximum efficiency.

Specific control activities that Garbanzo LLC has implemented in this area are described below:

- Background checks are performed on new hires, who are evaluated for competence in performing their job responsibilities at the time of hiring.
- Job positions are supported by job descriptions.
- New employees are required to acknowledge company policy and confidentiality related agreements upon hire and annually thereafter.
- Upon hire and annually thereafter, all employees must complete training courses covering basic information security practices.
- Performance evaluations for each employee are performed on an annual basis.
- If an employee violates the Code of Conduct in the employee handbook or the company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the company, the employee is subject to sanctions up to and including termination of employment.
- When a person is relieved of duties from the company, access to critical systems is made inaccessible in a timely manner

Risk Assessment

Garbanzo LLC’s risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. Garbanzo LLC identifies the underlying sources of risk, measures the impact on the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the Garbanzo Software Application, and the management has implemented various measures designed to manage these risks.

Garbanzo LLC believes that effective risk management is based on the following principles:

- Senior management’s commitment to the security of the Garbanzo Software Application
- The involvement, cooperation, and insight of all Garbanzo LLC staff
- Initiating risk assessments with discovery and identification of risks
- A thorough analysis of identified risks
- Commitment to the strategy and treatment of identified risks
- Communicating all identified risks to the senior management
- Encouraging all Garbanzo LLC staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the Garbanzo Software Application. Garbanzo LLC risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage, and services. The risk assessments also include an analysis of business/IT practices, procedures, and physical spaces as needed.

Risk assessments may be high-level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of Garbanzo LLC’s Information Security Officer and the department or individuals responsible for the area being assessed. All Garbanzo LLC staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff is further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

Garbanzo LLC uses a number of vendors to meet its business objectives. Garbanzo LLC understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

Garbanzo LLC employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, Garbanzo LLC assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support Garbanzo LLC’s commitments to its customers.

If a critical vendor is unable to provide a third-party security report or assessment, Garbanzo LLC management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix, which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, Garbanzo LLC identifies the specific risks that service commitments may not be met, and designs control necessary to address those risks. Garbanzo LLC’s management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the Company, as well as their potential impacts, likelihood, severity, and mitigating action.

Control Activities

Garbanzo LLC’s control activities are defined through its established policies and procedures which address individual risks associated with the achievement of the company's objectives. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions.

Policies serve as the basis for procedures. Control activities are deployed through policies that establish what is expected and procedures that put policies into action.

Monitoring

Garbanzo LLC management monitors control to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations, or a combination of the two.

Information and Communication Systems

Garbanzo LLC maintains a company-wide Information Security Policy, supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, Garbanzo LLC also has additional policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff via the company employee portal.

Significant Events and Conditions

Garbanzo LLC has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact on the software application.

3.5 Principal Service Commitments and System Requirements

Garbanzo LLC designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Garbanzo LLC makes to user entities, the AWS and Digital Ocean and regulations that govern its services, and the financial, operational, and compliance requirements that Garbanzo LLC has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. These principles include but are not limited to, the following:

- The fundamental design of Garbanzo LLC’s software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role;
- Garbanzo LLC implements various procedures and processes to control access to the production environment and the supporting infrastructure;

- Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics;
- Regular vulnerability scans over the system and network, and penetration tests over the production environment; and,
- Operational procedures for managing security incidents and breaches, including notification procedures.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Garbanzo LLC and user entities

Availability commitments include, but are not limited to, the following

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components;
- Responding to customer requests in a reasonably timely manner;
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities

Such requirements are communicated in Garbanzo LLC's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

3.6 Complementary Customer Control (CUEC)

Garbanzo LLC's controls related to Garbanzo LLC cover a subset of overall internal control for each user of the software application. The control objectives related to Garbanzo LLC cannot be achieved solely by the controls put in place by Garbanzo LLC; each customer's internal controls need to be considered along with Garbanzo LLC's controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

Related Criteria	CUEC Description
CC5.1 CC5.2 CC5.3 CC6.1	Customers are responsible for managing their organization's Garbanzo Software Application account as well as establishing any customized security solutions or automated processes through the use of setup features
CC5.2 CC6.3	Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their Garbanzo Software Application account

CC7.2 CC7.3 CC7.4	Customers are responsible for notifying Garbanzo LLC of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of Garbanzo Software Application.
CC8.1	Customers are responsible for any changes made to user and organization data stored within the Garbanzo Software Application.
CC7.2 CC7.3 CC7.4	Customers are responsible for communicating relevant security and availability issues and incidents to Garbanzo LLC through identified channels.

3.7 Complementary Subservice Organization Controls (CSOC)

Garbanzo LLC uses subservice organizations in support of its system. Garbanzo LLC's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over Garbanzo LLC to be achieved solely by Garbanzo LLC Therefore, user entity controls must be evaluated in conjunction with Garbanzo LLC's controls described in Section IV of this report, considering the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Garbanzo LLC periodically reviews the quality of the outsourced operations by various methods including

- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements

Subservice Organization	Applicable Criteria	CSOC Description
AWS and Digital Ocean	CC6.1 CC6.2 CC6.3 CC6.5 CC7.2	Logical access to the underlying network and virtualization management software for the cloud architecture is appropriate.
	CC6.4 CC6.5	Physical access and security to the data center facility are restricted to authorized personnel.
	CC6.4 A1.2	Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.
	A1.3	Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.
	A1.2	Policies and procedures to document repairs and modifications to the physical components of a facility including, but not limited to, hardware, walls, doors, locks, and other physical security components.
	C1.1	A defined Data Classification Policy specifies classification levels and control requirements in order to meet the company's commitments related to confidentiality.

	C1.2	A defined process is in place to sanitize and destroy hard drives and backup media containing customer data prior to leaving company facilities.
	CC6.1	Encryption methods are used to protect data in transit and at rest.

[Space intentionally left blank]

3.8 Applicable Trust Services Criteria and Related Controls

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
CONTROL ENVIRONMENT			
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values	SDC 1	Entity has a documented policy to define behavioral standards and acceptable business conduct.
		SDC 6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	SDC 24	Entity's Senior Management reviews and approves all company policies annually.
		SDC 25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		SDC 26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC 27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC 29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	SDC 2	Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.
		SDC 3	Entity has established procedures to communicate with staff about their roles and responsibilities.
		SDC 22	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.
		SDC 25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
		SDC 154	Entity has set up mechanism to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.
		SDC 396	Entity appoints a People Operations Officer to develop and drive all personnel related security strategies.
		SDC 397	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	SDC 4	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.
		SDC 5	Entity has established procedures to perform security risk screening of individuals prior to authorizing access.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives	SDC 7	Entity provides information security and privacy training to staff that is relevant for their job function.
		SDC 9	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their job responsibilities.
		SDC 12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC 383	Entity requires that all staff members complete Information Security Awareness training annually.
		SDC 387	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.
		SDC 388	Entity documents, monitors and retains individual training activities and records.
COMMUNICATION AND INFORMATION			
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control	SDC 11	Entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.
		SDC 13	Entity makes all policies and procedures available to all staff members for their perusal.
		SDC 14	Entity displays the most current information about its services on its website, which is

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
			accessible to its customers.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control	SDC 1	Entity has a documented policy to define behavioral standards and acceptable business conduct.
		SDC 6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC 13	Entity makes all policies and procedures available to all staff members for their perusal.
		SDC 15	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.
		SDC 383	Entity requires that all staff members complete Information Security Awareness training annually.
		SDC 387	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.
		SDC 388	Entity documents, monitors and retains individual training activities and records.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control	SDC 14	Entity displays the most current information about its services on its website, which is accessible to its customers.
		SDC 16	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.
RISK ASSESSMENT			
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives	SDC 18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.
CC3.2	COSO Principle 7: The entity	SDC 6	Entity has established procedures for new staff to acknowledge applicable company

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
	identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed		policies as a part of their onboarding.
		SDC 18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.
		SDC 19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC 21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives	SDC 20	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control	SDC 18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.
		SDC 19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC 21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
MONITORING ACTIVITIES			
CC4.1	COSO Principle 16*:* The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and	SDC 22	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.
		SDC 23	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
	functioning		stakeholders.
		SDC 24	Entity's Senior Management reviews and approves all company policies annually.
		SDC 25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		SDC 26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC 27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC 29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.
		SDC 30	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.
		SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC 56	Entity tracks all vulnerabilities, and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC 154	Entity has set up mechanism to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.
		SDC 389	Entity periodically updates and reviews the inventory of systems as a part of installations, removals and system updates.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and	SDC 15	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.
		SDC 23	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
	the board of directors, as appropriate	SDC 24	Entity's Senior Management reviews and approves all company policies annually.
		SDC 25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		SDC 63	Entity identifies vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third party service provider.
CONTROL ACTIVITIES			
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels	SDC 31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
		SDC 32	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.
		SDC 105	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives	SDC 23	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC 24	Entity's Senior Management reviews and approves all company policies annually.
		SDC 25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
		SDC 26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.
		SDC 27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.
		SDC 28	Entity's Infosec officer reviews and approves the list of people with access to production console annually
		SDC 29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
			Report" annually.
		SDC 30	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.
		SDC 31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action	SDC 6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	Entity has established procedures for staff to acknowledge applicable company policies periodically.
		SDC 13	Entity makes all policies and procedures available to all staff members for their perusal.
		SDC 31	Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.
Logical and Physical Access Controls			
CC6.1	*The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives*	SDC 33	Entity has documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.
		SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorised personnel on an individual need or for a predefined role.
		SDC 38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
		SDC 42	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC 43	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC 108	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
			roles have changed
		SDC 135	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal
CC6.2	*Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized*	SDC 33	Entity has documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.
		SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorised personnel on an individual need or for a predefined role.
		SDC 35	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.
CC6.3	*The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives*	SDC 33	Entity has documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.
		SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorised personnel on an individual need or for a predefined role.
		SDC 35	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.
		SDC 37	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.
		SDC 42	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
		SDC 43	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
			access to the critical systems is restricted to only those individuals who require such access to perform their job functions.
CC6.4	*The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives*	N/A	The entity does not have any physical offices or physical data centers. Hence, not applicable.
CC6.5	*The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives*	SDC 48	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.
CC6.6	*The entity implements logical access security measures to protect against threats from sources outside its system boundaries*	SDC 38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.
		SDC 39	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor-authentication.
		SDC 44	Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.
		SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorised access.
		SDC 46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
			remote devices prior to the establishment of the internal connection.
		SDC 47	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.
		SDC 50	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.
		SDC 104	Entity has documented policy and procedures for endpoint security and related controls.
		SDC 141	Entity requires that all critical endpoints are encrypted to protect them from unauthorised access
		SDC 390	Entity develop, document, and maintain an inventory of organizational endpoint systems, including all necessary information to achieve accountability.
CC6.7	*The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives*	SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorised access.
		SDC 49	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.
		SDC 51	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.
		SDC 52	Entity develop, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.
		SDC 100	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment
		SDC 106	Entity has a documented policy to manage encryption and cryptographic protection controls.
		SDC 141	Entity requires that all critical endpoints are encrypted to protect them from unauthorised access
CC6.8	*The entity implements controls to prevent or detect and act*	SDC 46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
	upon the introduction of unauthorized or malicious software to meet the entity's objectives		the internal connection.
		SDC 50	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.
System Operations			
CC7.1	*To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities*	SDC 61	Entity's infrastructure is configured to review and analyse audit events to detect anomalous or suspicious activity and threats
		SDC 62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
		SDC 391	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.
		SDC 392	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident
CC7.2	*The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events*	SDC 61	Entity's infrastructure is configured to review and analyse audit events to detect anomalous or suspicious activity and threats
		SDC 62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
		SDC 391	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.
		SDC 392	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident
CC7.3	*The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes*	SDC 23	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC 46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
	actions to prevent or address such failures	SDC 54	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.
		SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
		SDC 56	Entity tracks all vulnerabilities, and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC 61	Entity's infrastructure is configured to review and analyse audit events to detect anomalous or suspicious activity and threats
		SDC 62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
		SDC 391	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.
		SDC 392	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident
CC7.4	*The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate*	SDC 23	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.
		SDC 53	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.
		SDC 54	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.
		SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.
CC7.5	*The entity identifies, develops, and implements activities to*	SDC 393	Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
	recover from identified security incidents		
Change Management			
CC8.1	*The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures_to meet its objectives*	SDC 52	Entity develop, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.
		SDC 56	Entity tracks all vulnerabilities, and remediates them as per the policy and procedure defined to manage vulnerabilities.
		SDC 64	Entity has documented policies and procedures to manage changes to its operating environment.
		SDC 65	Entity has procedures to govern changes to its operating environment.
		SDC 66	Entity has established procedures for approval when implementing changes to the operating environment.
Risk Mitigation			
CC9.1	*The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions*	SDC 18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.
		SDC 19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.
		SDC 67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements
CC9.2	*The entity assesses and manages risks associated with vendors and business partners*	SDC 21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.
		SDC 67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements
		SDC 68	Entity has a documented policy and

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
			procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors
Additional Criteria for Availability			
A1.1	*The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives*	SDC 62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.
A1.2	*The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives*	SDC 59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives, and verifies the integrity of these backups.
		SDC 60	Entity tests backup information periodically to verify media reliability and information integrity.
		SDC 394	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems
A1.3	*The entity tests recovery plan procedures supporting system recovery to meet its objectives*	SDC 60	Entity tests backup information periodically to verify media reliability and information integrity.
		SDC 97	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.
Additional Criteria for Confidentiality			
C1.1	*The entity identifies and maintains confidential information to*	SDC 6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.
		SDC 12	Entity has established procedures for staff to acknowledge applicable company policies

TSC Ref	Criteria	Control	Control Activity as specified by Garbanzo LLC
	meet the entity's objectives related to confidentiality		periodically.
		SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorised access.
		SDC 49	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.
		SDC 69	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems
		SDC 70	Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification
C1.2	*The entity disposes of confidential information to meet the entity's objectives related to confidentiality*	SDC 48	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.
		SDC 71	Entity has a documented policy outlining guidelines for the disposal and retention of information.

[Space intentionally left blank]

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR: TEST OF CONTROLS

4. Information Provided by Service Auditor Except for Applicable Trust Services Criteria and Controls

4.1 Objective of Our Examination

This report is intended to provide interested parties with information about the controls at Garbanzo LLC that may affect the processing of user organizations' transactions and also to provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user organizations, is intended to assist user auditors in (1) planning the audit of user organizations' financial statements and in (2) assessing control risk for assertions in user organizations' financial statements that may be affected by controls at Garbanzo LLC

Our testing of Garbanzo LLC's controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in system description but not included in the aforementioned matrices, or to controls that may be in effect at user organizations. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organization. If certain complementary controls are not in place at user organizations, Garbanzo LLC's controls may not compensate for such weaknesses.

4.2 Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Garbanzo LLC our procedures included tests of the following relevant elements of Garbanzo LLC's control environment:

1. Environment
2. Internal Risk Assessment
3. Information and Communication
4. Control Activities
5. Monitoring

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Garbanzo LLC activities and operations, inspection of Garbanzo LLC documents and records, and re-performance of the application of Garbanzo LLC controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

4.3 Applicable Trust Services Criteria, Controls, Tests of Operating Effectiveness, and Results of Tests

Our tests were designed to examine Garbanzo LLC description of the system related to Garbanzo LLC as well as the suitability of the design and operating effectiveness of controls for a representative number of samples for the period from February 28, 2024 to June 06, 2024.

In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) types of available evidential matter, (c) nature of the trust services principles and criteria to be achieved and (d) expected efficiency and effectiveness of the test.

Testing the accuracy and completeness of information provided by Garbanzo LLC is also a component of the testing procedures performed. Information we are utilizing as evidence may include, but is not limited to:

1. Standard ‘out of the box’ reports as configured within the system
2. Parameter-driven reports generated by Garbanzo LLC
3. Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
4. Spreadsheets that include relevant information utilized for the performance or testing of a control
5. Garbanzo LLC-prepared analyses, schedules, or other evidence manually prepared and utilized by the Company

While these procedures are not specifically called out in the test procedures listed in this section, they are completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Garbanzo LLC

Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and re-performance of controls surrounding and provided by Garbanzo LLC Our tests of controls were performed on controls as they existed for the period from February 28, 2024 to June 06, 2024 and were applied to those controls relating to the trust services principles and criteria.

Tests performed of the operational effectiveness of controls are described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Examination of Documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Re-performance of Monitoring Activities or Manual Controls	Obtained documents used in the monitoring activity or manual control activity and independently re-performed the procedures. Compared any exception items identified with those identified by the responsible control owner.
Re-performance of Programmed Processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

4.4 Testing Procedures Performed by Independent Service Auditor

In addition to the tests listed below for each control specified by Garbanzo LLC, ascertained through inquiry with management and the control owner that each control activity listed below operated as described for the period from February 28, 2024 to June 06, 2024.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC1.1 CC2.2	SDC 1	Entity has a documented policy to define behavioral standards and acceptable business conduct.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had a documented policy to define behavioral standards and acceptable business conduct.	No Exceptions Noted.
CC1.3	SDC 2	Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity maintained an organizational structure to define authorities, facilitate information flow and establish responsibilities.	No Exceptions Noted.
CC1.3	SDC 3	Entity has established procedures to communicate with staff about their roles and responsibilities.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had established procedures to communicate with staff about their roles and responsibilities.	No Exceptions Noted.
CC1.4	SDC 4	Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had procedures to ensure that all security-related positions were staffed by qualified individuals who had the necessary skill set.	No Exceptions Noted.
CC1.4	SDC 5	Entity has established procedures to perform security risk screening of individuals prior to authorizing access.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had established procedures to perform security risk	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
			screening of individuals prior to authorizing access.	
C1.1 CC1.1 CC2.2 CC3.2 CC5.3	SDC 6	Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.	No Exceptions Noted.
CC1.5	SDC 7	Entity provides information security and privacy training to staff that is relevant for their job function.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity provided information security and privacy training to staff that is relevant for their job function.	No Exceptions Noted.
CC1.5	SDC 9	Entity requires that all employees in client serving, IT, Engineering and Information Security roles are periodically evaluated regarding their job responsibilities.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity required that all employees in client serving, IT, Engineering and Information Security roles were periodically evaluated regarding their job responsibilities.	No Exceptions Noted.
CC2.1	SDC 11	Entity systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity systems generated information that was reviewed and evaluated to determine impacts to the functioning of internal controls.	No Exceptions Noted.
C1.1 CC1.1 CC1.5 CC2.2 CC5.3	SDC 12	Entity has established procedures for staff to acknowledge applicable company policies periodically.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had established procedures for staff to acknowledge applicable company policies periodically.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC2.1 CC2.2 CC5.3	SDC 13	Entity makes all policies and procedures available to all staff members for their perusal.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity made all policies and procedures available to all staff members for their perusal.	No Exceptions Noted.
CC2.1 CC2.3	SDC 14	Entity displays the most current information about its services on its website, which is accessible to its customers.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity displayed the most current information about its services on its website, which is accessible to its customers.	No Exceptions Noted.
CC2.2 CC4.2	SDC 15	Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there were problems.	No Exceptions Noted.
CC2.3	SDC 16	Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there were problems.	No Exceptions Noted.
CC3.1 CC3.2 CC3.4 CC9.1	SDC 18	Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity performed a formal risk assessment exercise annually, as per documented guidelines and procedures,	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
			to identify threats that could impair systems' security commitments and requirements.	
CC3.2 CC3.4 CC9.1	SDC 19	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether each risk was assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks were mapped to mitigating factors that address some or all of the risk.	No Exceptions Noted.
CC3.3	SDC 20	Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity considered the potential for fraud when assessing risks. This was an entry in the risk matrix.	No Exceptions Noted.
CC3.2 CC3.4 CC9.2	SDC 21	Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity performed a formal vendor risk assessment exercise annually to identify vendors that were critical to the systems' security commitments and requirements.	No Exceptions Noted.
CC1.3 CC4.1	SDC 22	Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether Entity's Senior Management assigned the role of Information Security Officer who was delegated to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC4.1 CC4.2 CC5.2 CC7.3 CC7.4	SDC 23	Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether Entity used Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	No Exceptions Noted.
CC1.2 CC4.1 CC4.2 CC5.2	SDC 24	Entity's Senior Management reviews and approves all company policies annually.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management reviewed and approved all company policies annually.	No Exceptions Noted.
CC1.2 CC1.3 CC4.1 CC4.2 CC5.2	SDC 25	Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management reviewed and approved the state of the Information Security program including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	No Exceptions Noted.
CC1.2 CC4.1 CC5.2	SDC 26	Entity's Senior Management reviews and approves the Organizational Chart for all employees annually.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management reviewed and approved the Organizational Chart for all employees annually.	No Exceptions Noted.
CC1.2 CC4.1 CC5.2	SDC 27	Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management reviewed and approved the "Risk Assessment Report" annually.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC5.2	SDC 28	Entity's Infosec officer reviews and approves the list of people with access to production console annually	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Infosec officer reviewed and approved the list of people with access to production console annually.	No Exceptions Noted.
CC1.2 CC4.1 CC5.2	SDC 29	Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management reviewed and approved the "Vendor Risk Assessment Report" annually.	No Exceptions Noted.
CC4.1 CC5.2	SDC 30	Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity reviewed and evaluated all subservice organizations periodically, to ensure commitments to Entity's customers were met.	No Exceptions Noted.
CC5.1 CC5.2 CC5.3	SDC 31	Entity has developed a set of policies that establish expected behavior with regard to the Company’s control environment.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had developed a set of policies that established expected behavior with regard to the Company’s control environment.	No Exceptions Noted.
CC5.1	SDC 32	Entity's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management segregated responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	No Exceptions Noted.
CC6.1 CC6.2 CC6.3	SDC 33	Entity has documented policy and procedures to manage Access Control and an accompanying process to register and	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
		authorize users for issuing system credentials which grant the ability to access the critical systems.	documented policy and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which granted the ability to access the critical systems.	
CC6.1 CC6.2 CC6.3	SDC 34	Entity ensures that logical access provisioning to critical systems requires approval from authorised personnel on an individual need or for a predefined role.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity ensured that logical access provisioning to critical systems required approval from authorised personnel on an individual need or for a predefined role.	No Exceptions Noted.
CC6.2 CC6.3	SDC 35	Entity ensures logical access that is no longer required in the event of a termination is made inaccessible in a timely manner.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity ensured logical access that is no longer required in the event of a termination was made inaccessible in a timely manner.	No Exceptions Noted.
CC6.3	SDC 37	Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity ensured that access to the production databases was restricted to only those individuals who required such access to perform their job functions.	No Exceptions Noted.
CC6.1 CC6.6	SDC 38	Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity ensured that the production databases access and Secure Shell access to infrastructure entities were protected from public internet access.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC6.6	SDC 39	Entity requires that all staff members with access to any critical system is protected with a secure login mechanism such as Multifactor-authentication.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity required that all staff members with access to any critical system was protected with a secure login mechanism such as Multifactor-authentication.	No Exceptions Noted.
CC6.1 CC6.3	SDC 42	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management or the Information Security Officer periodically reviewed and ensured that access to the critical systems was restricted to only those individuals who required such access to perform their job functions.	No Exceptions Noted.
CC6.1 CC6.3	SDC 43	Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's Senior Management or the Information Security Officer periodically reviewed and ensured that administrative access to the critical systems was restricted to only those individuals who require such access to perform their job functions.	No Exceptions Noted.
CC6.6	SDC 44	Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity ensured that endpoints with access to critical servers or data were protected by malware-protection software.	No Exceptions Noted.
C1.1 CC6.6	SDC 45	Where applicable, Entity ensures that endpoints with access to critical servers or	Obtained and inspected the supporting evidence on the Sprinto Platform to	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC6.7		data must be encrypted to protect from unauthorised access.	ascertain whether the Entity ensured that endpoints with access to critical servers or data were encrypted to protect from unauthorised access.	
CC6.6 CC6.8 CC7.3	SDC 46	Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	No Exceptions Noted.
CC6.6	SDC 47	Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity ensured that endpoints with access to critical servers or data were configured to auto-screen-lock after 15 minutes of inactivity.	No Exceptions Noted.
C1.2 CC6.5	SDC 48	Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had a documented policy that provided guidance on decommissioning of information assets that contain classified information.	No Exceptions Noted.
C1.1 CC6.7	SDC 49	Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.	No Exceptions Noted.
CC6.6 CC6.8	SDC 50	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether every Production host was	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
		cloud provider.	protected by a firewall with a deny-by-default rule. Deny by default rule set was a default on the Entity's cloud provider.	
CC6.7	SDC 51	User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether user access to the entity's application was secured using https (TLS algorithm) and industry standard encryption.	No Exceptions Noted.
CC6.7 CC8.1	SDC 52	Entity develop, document, and maintain an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity developed, documented, and maintained an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	No Exceptions Noted.
CC7.4	SDC 53	Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had established a policy and procedure which included guidelines to be undertaken in response to information security incidents.	No Exceptions Noted.
CC7.3 CC7.4	SDC 54	Entity maintains a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity maintained a record of information security incidents, its investigation and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.	No Exceptions Noted.
CC4.1 CC7.3 CC7.4	SDC 55	Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity identified	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
			vulnerabilities on the Company platform through the execution of regular vulnerability scans.	
CC4.1 CC7.3 CC8.1	SDC 56	Entity tracks all vulnerabilities, and remediates them as per the policy and procedure defined to manage vulnerabilities.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity tracked all vulnerabilities, and remediated them as per the policy and procedure defined to manage vulnerabilities.	No Exceptions Noted.
A1.2	SDC 59	Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives, and verifies the integrity of these backups.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity backed up relevant user and system data regularly to meet recovery time and recovery point objectives, and verified the integrity of these backups.	No Exceptions Noted.
A1.2 A1.3	SDC 60	Entity tests backup information periodically to verify media reliability and information integrity.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity tested backup information periodically to verify media reliability and information integrity.	No Exceptions Noted.
CC7.1 CC7.2 CC7.3	SDC 61	Entity's infrastructure is configured to review and analyse audit events to detect anomalous or suspicious activity and threats	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's infrastructure was configured to review and analyse audit events to detect anomalous or suspicious activity and threats.	No Exceptions Noted.
A1.1 CC7.1 CC7.2 CC7.3	SDC 62	Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had set up methods to continuously monitor critical assets to generate capacity alerts to ensure	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
			optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	
CC4.2	SDC 63	Entity identifies vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third party service provider.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity identified vulnerabilities on the company platform through annual penetration testing exercise conducted by a qualified third party service provider.	No Exceptions Noted.
CC8.1	SDC 64	Entity has documented policies and procedures to manage changes to its operating environment.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had documented policies and procedures to manage changes to its operating environment.	No Exceptions Noted.
CC8.1	SDC 65	Entity has procedures to govern changes to its operating environment.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether Entity had procedures to govern changes to its operating environment.	No Exceptions Noted.
CC8.1	SDC 66	Entity has established procedures for approval when implementing changes to the operating environment.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had established procedures for approval when implementing changes to the operating environment.	No Exceptions Noted.
CC9.1 CC9.2	SDC 67	Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate Entity's service commitments and system requirements	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had documented policies and procedures that describe how to identify risks to business objectives and how those risks were	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
			assessed and mitigated. The objectives incorporated Entity's service commitments and system requirements.	
CC9.2	SDC 68	Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had a documented policy and procedures to manage Vendors / third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	No Exceptions Noted.
C1.1	SDC 69	Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had a documented Information Security Policy that governed the confidentiality, integrity, and availability of information systems.	No Exceptions Noted.
C1.1	SDC 70	Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity performed physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	No Exceptions Noted.
C1.2	SDC 71	Entity has a documented policy outlining guidelines for the disposal and retention of information.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had a documented policy outlining guidelines for the disposal and retention of information.	No Exceptions Noted.
A1.3	SDC 97	Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had procedures to conduct regular tests and exercises that	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
			determined the effectiveness and the readiness to execute the contingency plan.	
CC6.7	SDC 100	Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity ensured that customer data used in non-Production environments requires the same level of protection as the production environment	No Exceptions Noted.
CC6.6	SDC 104	Entity has documented policy and procedures for endpoint security and related controls.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had documented policy and procedures for endpoint security and related controls.	No Exceptions Noted.
CC5.1	SDC 105	Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity established guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	No Exceptions Noted.
CC6.7	SDC 106	Entity has a documented policy to manage encryption and cryptographic protection controls.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had a documented policy to manage encryption and cryptographic protection controls.	No Exceptions Noted.
CC6.1	SDC 108	Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity used Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles were changed.	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC6.1	SDC 135	Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had documented guidelines to manage passwords and secure login mechanisms and made them available to all staff members on the company employee portal.	No Exceptions Noted.
CC6.6 CC6.7	SDC 141	Entity requires that all critical endpoints are encrypted to protect them from unauthorised access	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity required that all critical endpoints were encrypted to protect them from unauthorised access.	No Exceptions Noted.
CC1.3 CC4.1	SDC 154	Entity has set up mechanism to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had set up mechanism to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	No Exceptions Noted.
CC1.5 CC2.2	SDC 383	Entity requires that all staff members complete Information Security Awareness training annually.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity required all staff members to complete Information Security Awareness training annually.	No Exceptions Noted.
CC1.5 CC2.2	SDC 387	Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.	No Exceptions Noted.
CC1.5 CC2.2	SDC 388	Entity documents, monitors and retains individual training activities and records.	Obtained and inspected the supporting evidence on the Sprinto Platform to	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
			ascertain whether the Entity documented, monitored and retained individual training activities and records.	
CC4.1	SDC 389	Entity periodically updates and reviews the inventory of systems as a part of installations, removals and system updates.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity periodically updated and reviewed the inventory of systems as a part of installations, removals and system updates.	No Exceptions Noted.
CC6.6	SDC 390	Entity develop, document, and maintain an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity developed, documented, and maintained an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	No Exceptions Noted.
CC7.3 CC7.1 CC7.2	SDC 391	Entity has a documented policy and procedures to establish guidelines on managing technical vulnerabilities.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had documented policy and procedures to establish guidelines on managing technical vulnerabilities.	No Exceptions Noted.
A1.2 A1.3 CC7.5	SDC 392	Entity has documented guidelines to manage Disaster Recovery that establishes guidelines and procedures for continuing business operations in case of a disruption or a security incident	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity had documented guidelines to manage Disaster Recovery that established guidelines and procedures for continuing business operations in case of a disruption or a security incident.	No Exceptions Noted.
A1.2 A1.3	SDC 393	Entity has documented policies and procedures that establish guidelines for	Obtained and inspected the supporting evidence on the Sprinto Platform to	No Exceptions Noted.

TSC Ref	Control#	Control Activities as specified by Garbanzo LLC	Test Procedures performed	Results of Test
CC7.5		continuing business operations and facilitate the application of contingency planning controls.	ascertain whether the Entity had documented policies and procedures that established guidelines for continuing business operations and facilitate the application of contingency planning controls.	
CC7.1 CC7.2 CC7.3	SDC 394	Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity's infrastructure was configured to generate audit events for actions of interest related to security for all critical systems.	No Exceptions Noted.
CC1.3	SDC 396	Entity appoints a People Operations Officer to develop and drive all personnel related security strategies.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity appointed a People Operations Officer to develop and drive all personnel related security strategies.	No Exceptions Noted.
CC1.3	SDC 397	Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	Obtained and inspected the supporting evidence on the Sprinto Platform to ascertain whether the Entity appointed a Compliance Program Manager who was delegated the responsibility of planning and implementing the internal control environment.	No Exceptions Noted.

[End of the report]